Understanding Terrorist Network Topologies and Their Resilience Against Disruption

Lindelauf, R.; Borm, P.E.M.; Hamers, H.J.M.

Publication date:
2009

CentER

Discussion Paper

No. 2009–85

UNDERSTANDING TERRORIST NETWORK TOPOLOGIES AND THEIR RESILIENCE AGAINST DISRUPTION

By Roy Lindelauf, Peter Borm, Herbert Hamers

November 2009

ISSN 0924-7815

Tilburg University

Understanding terrorist network topologies and their resilience against disruption

Roy Lindelauf [a,b] Peter Borm [b] Herbert Hamers [b]

November 4, 2009

Abstract

This article investigates the structural position of covert (terrorist or criminal) networks. Using the secrecy versus information tradeoff characterization of covert networks it is shown that their network structures are generally not small-worlds, in contradistinction to many overt social networks. This finding is backed by empirical evidence concerning Jemaah Islamiyah's Bali bombing and a heroin distribution network in New York. The importance of this finding lies in the strength such a topology provides. Disruption and attack by counterterrorist agencies often focuses on the isolation and capture of highly connected individuals. The remarkable result is that these covert networks are well suited against such targeted attacks as shown by the resilience properties of secrecy versus information balanced networks. This provides an explanation of the survival of global terrorist networks and food for thought on counterterrorism strategy policy.

Keywords: terror networks; terrorist cells; network structure; counterterrorism.

JEL classification: C02, C79.

As researchers have begun to unravel the structure and dynamics of many different social, biological and other complex networks (Strogatz 2001, Jasny et al. 2003, Newman et al. 2006)) it is realized that the study of criminal and terrorist networks can also benefit from insights thus obtained (Zacharias et al. 2008). Typically research on terrorist or criminal networks, i.e., covert networks, considers destabilization strategies (Farley 2003, Carley 2006), organizational characterizations (McCormick & Owen 2000, Enders and Su 2007, Morselli et al. 2007) and methods for key player identification (Sparrow 1991, Borgatti 2002). Network oriented research in this domain is ordinarily done by either assuming a fixed network topology or by the use of empirical historical data (Magouirk 2008, Asal et al. 2007). However, data on this topic is often inaccurate and anecdotal due to the widespread secrecy surrounding governmental data-sets. Mathematical models

[a]Military Operational Art & Science, Netherlands Defense Academy, P.O.Box 90002, 4800 PA Breda, The Netherlands. E-mail: rha.lindelauf.01@nlda.nl

[b]CentER and Department of Econometrics and OR, Tilburg University, P.O.Box 90153, 5000 LE Tilburg, The Netherlands.

provide an alternative method for gaining insight into covert organizational structures. Once data becomes available these models can be evaluated and adjusted if necessary.

For many types of (overt) networks the position of their connection topology between the extremes of order and randomness has been established (Watts and Strogatz 1998, Watts 2004). However, little is known about the exact position of the connection topology of covert networks, and consequently about their resilience against disruption. The current study shows where covert networks are positioned by making use of their topological characterization as secrecy influenced communication structures (Lindelauf et al. 2009a/b). We find that the common characterization of social systems as small-world networks is generally not applicable to covert networks. This phenomenon can be explained by the fundamental dilemma such organizations have to solve: how to efficiently coordinate and exercise control while at the same time remaining secret. We corroborate our results with empirical findings of Jemaah Islamiyah's bombing of a Bali nightclub (Koschade 2006) and the active core of a heroin distribution network in New York City (Natarajan 2006). In addition we show that a covert network topology is strongly resilient against disruption strategies focused on capturing and isolating highly connected individuals, partly explaining the difficulties in disrupting current terror networks.

Theoretical results and empirical investigations indicate that terrorist organizations have to make a trade-off between efficient coordination and control on the one hand and maintaining secrecy on the other. For instance Enders and Su (2007) model the process by which terrorists select 'between the competing ends of security versus the unbridled flow of information'. They argue that rational terrorists will attempt to counter increased efforts at infiltration and restructure themselves to be less penetrable, often by adopting certain network structures. That terrorist organizations take secrecy explicitly into account is well known: in a video lecture Mousab al Suri (an alleged Al Qaeda affiliate that was captured in November 2005) indicates that certain network structures should be avoided to ensure the secrecy of the organization (Bergen 2006). Terrorists operating according to networked organizational forms are also observed in practice. For instance the Nov. 26 Mumbai attack showed tactical commanders and individual team members using satellite and cell phones to connect to strategic commanders out of theatre. Multiple teams consisting of several individuals were able to communicate and direct each other as the attacks progressed. What sets apart such attacks is not the use of technology per se but the networked mode

of operation that it enables. The organizational form of these attackers is not easily characterized as being 'hierarchical' or 'decentralized'. However, what is clear is that terrorist, insurgent and criminal organizations are increasingly able to cross borders, engage in fluent relationships and 'swarm' their objectives to achieve their goals. The underlying mechanism to all these operations is the networked topology: information is exchanged on communication networks, weapons diffuse through trafficking networks and Shura councils meet in affiliation networks. It is therefore of paramount importance to understand these network structures.

Lindelauf et al. (2009a) introduce a multi-objective optimization framework to analyze the structure of terrorist networks taking the secrecy versus information tradeoff into account. That this tradeoff exists is intuitively clear: if everybody in the covert organization knows everybody else, then the security risk to the organization is very high because the exposure of an individual potentially exposes the entire organization. On the other hand, a very sparsely connected organizational network topology is difficult to coordinate and control, simply because efficient communication between individuals in such an organization is hard. We capture these critical considerations by use of an information measure I, a secrecy measure S, and a balanced trade-off measure μ. A detailed description of the methodology used can be found in the the appendix. The information measure I reflects the fact that the ability to transfer information between individuals in a network is inversely proportional to the number of edges in the shortest path between those individuals. On the other hand, the secrecy measure S reflects the fraction of individuals in the network that is expected to remain unexposed upon capture of individuals according to a realistically chosen probability distribution. Finally the total performance of a covert organization in dealing with the information versus secrecy trade-off dilemma is reflected by the multi-objective optimization based function $\mu = SI$. The higher the value of μ a network attains, the better it does in balancing secrecy and information.

Terrorist networks evolve, i.e., 'it would be naive to think that terrorists and their networks would remain invariant to measures designed to track and infiltrate the inner workings of their organizations' (Enders and Su 2007). To what kind of structures do these terrorist networks evolve? Clearly, we argue that the proactive counterterrorism activities after 9/11 have resulted in terrorist networks adopting more decentralized, non-hierarchical networks, i.e., they have taken secrecy explicitly into account as design parameter. Thus these terrorist networks are a very special

subset of general social networks about which a great deal is known (see for instance Wasserman and Faust 1994). For instance it is well known that many social networks can be characterized as small-worlds, i.e., most individuals in the network can be reached by a small number of steps. The evidence concerning terrorist network structures however is often anecdotal, providing an impetus for the development of theoretical models of covert networks. The aim of this article is therefore to analyze the structure of secrecy influenced terrorist networks, investigate their small-world properties and the resulting consequences on their survivability properties. The next section discusses the application of the secrecy versus information tradeoff characterization of terrorist networks to the analysis of their small-world structure. The important insight is that such terrorist networks do not appear to be small-worlds. A fact that can be motivated from a secrecy standpoint. In addition we will present empirical proof of this claim. Next we investigate the resilience of these terrorist network structures against disruption. We find that such network structures perform well against disruption, actually they outperform common social networks in case of targeted attacks. A fact that should have profound implications for counterterrorist strategies.

Small-world network analysis

Watts and Strogatz (1998) quantified small-worlds as networks with low characteristic path length L and high clustering coefficient C relative to random networks with the same number of vertices. The characteristic path length L is a global property that measures the typical separation between two individuals in the network. Obviously the characteristic path length L will be inversely related to the information measure I. This because a high separation between terrorists in the network will make it difficult for them to coordinate and control as reflected by a low information measure. The clustering coefficient C, a local property, measures the cliqueshness of a typical neighborhood. In many social networks an individual's friends are also friends among each other. Clearly, in covert networks this in general will not be the case because too many interconnections among individuals will degrade the secrecy of such an organization. The clustering coefficient C is based on the number of edges that exist between the neighbors of each vertex.

It is generally argued that covert organizations facing an exogenous threat transform into hybrid network structures that lie somewhere in between sparse networks (such as the star, ring, lattice or path) and the complete network in which everybody is connected to everybody else (Arquilla

and Ronfeldt 2001). To simulate this transformation we interpolate between regular networks and the complete network and for each instance establish the optimality of the resulting network with regard to the secrecy versus information tradeoff characterization. To investigate whether the small-world characterization of various social networks also holds true for covert networks, we thus generate intermediate hybrid networks. Our procedure starts with an initial network (a star, ring, path or lattice) and with a probability p that each vacant edge is added. For fixed values of p several indicators relating to the small-world structure (L, C) and the secrecy versus information tradeoff (μ) of the network are computed and averaged over 20 realizations. In Fig.1 we plot the normalized values of L, C and μ versus p for each of the four possible initial networks. It can be seen that the maximum value of μ, indicating approximate optimal covert network structures, is typically not attained at low characteristic path lengths and high clustering coefficients, features that characterize small-world networks. For instance, if the initial graph equals the path graph (Fig. 1 top right), then it can be seen that μ attains its maximum around $p = 0.09$, where the value of L is small and C does not attain a high value. In particular, the tiny fraction of shortcuts that suffices to create small-worlds, although increasing the ability to communicate, increases the security risk to a covert network. Clearly covert networks favor low clustering because this is in the interest of secrecy whereas low characteristic path lengths ensure the necessary communication and control abilities.

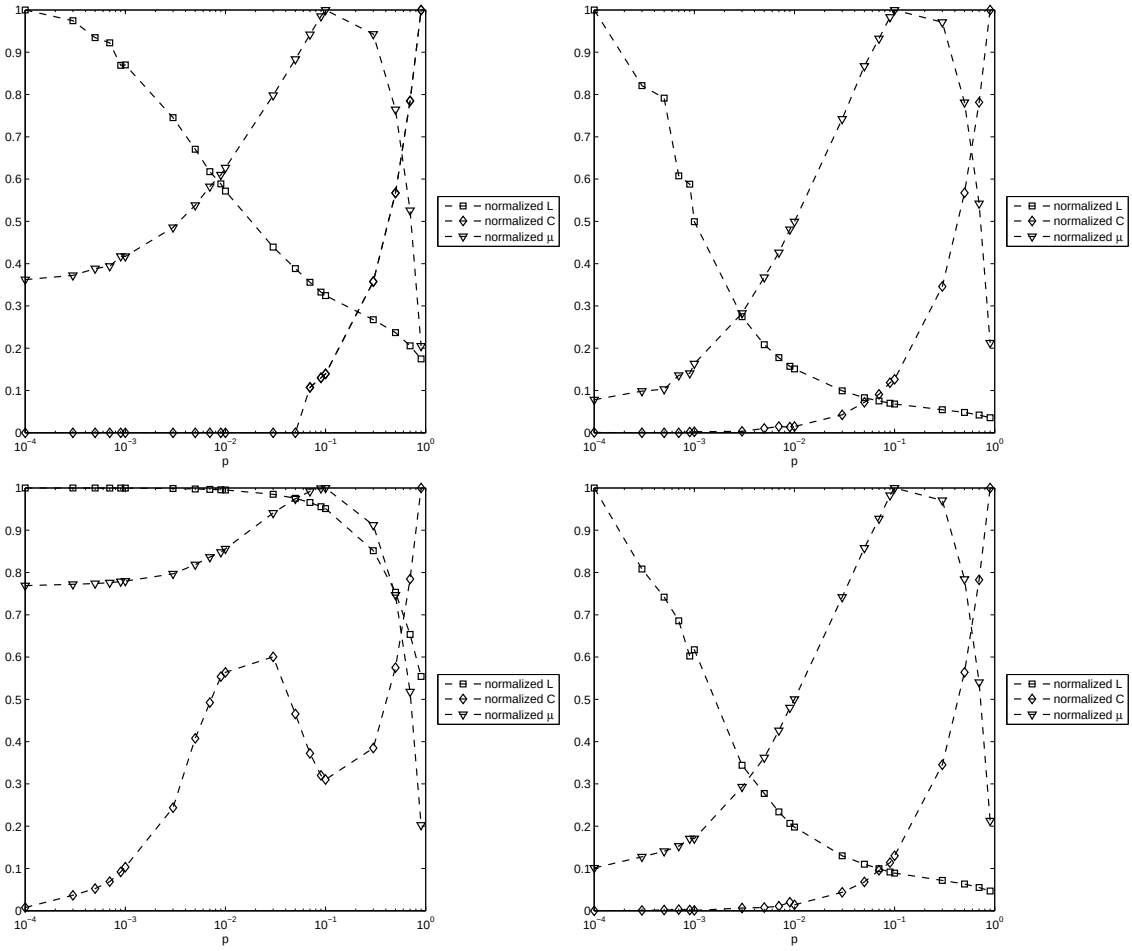

Figure 1: Normalized characteristic path length L, clustering coefficient C and performance measure μ as a function of the probability p with which each vacant edge is added to an initial network which is a lattice (top left), path (top right), star (bottom left) or ring (bottom right). All networks have 100 vertices and L, C and μ are averaged over 20 realizations for each of the values for p.

Empirical examples

Our simulation shows that the small-world phenomenon is not characteristic of theoretically optimal covert networks. To obtain additional evidence we compute the characteristic path length and clustering coefficient for empirical covert networks: a heroin distribution network in New York city and the Jemaah Islamiyah cell responsible for the Bali bombings in 2002. We compare these values to the characteristic path length and clustering coefficient of a graph with the same number of vertices in which every possible edge occurs independently with probability $p = \frac{1}{2}$, i.e., a random graph. To compare these outcomes with networks that are small-worlds we present an empirical example of a film-actor network (Watts and Strogatz 1998). It can be seen that both empirical covert networks do not show the small-world phenomenon because their characteristic path lengths as well as clustering coefficients are comparable to those of a random network (table 1). The film actor network however is a small-world: its characteristic path length is of similar order as the random graph on the same number of nodes whereas its clustering is much higher.

	L_{actual}	L_{random}	C_{actual}	C_{random}
Heroin Network	4.74	4.93	0.44	0.13
Jemaah Islamiyah	3.18	3.11	0.89	0.46
Film actors	3.65	2.99	0.79	0.00027

Table 1: Comparison of characteristic path lengths and clustering coefficients of two empirical covert networks and an overt empirical network (film actors) and 100.000 randomly generated graphs with the same number of vertices.

It is also interesting to investigate whether these empirical covert networks optimize their structure according to the theoretical framework on the secrecy versus information tradeoff dilemma. Therefore we compute μ for both empirical covert networks (μ_{he} and μ_{ji} respectively) and we approximate the optimal value of μ on networks of the same order (μ_{he}^{opt} and μ_{ji}^{opt} respectively). We find that $\frac{\mu_{he}}{\mu_{he}^{opt}} = \frac{0.33}{0.39} = 0.85$ and that $\frac{\mu_{ji}}{\mu_{ji}^{opt}} = \frac{0.28}{0.38} = 0.74$. We may conclude that both networks attain empirical values for μ that are close to optimal and hence correspond to the region (Fig. 1) within which the existence of a possible small-world structure is contradicted. Thus we obtain further evidence for the fact that covert organizations are not small-worlds. In the next section we will explain the advantage of adopting structures differing from small-worlds.

Covert network resilience

To counter the terrorist threat it is essential to focus on the terrorists (Sageman 2008). Generally speaking, in countering a covert network, the removal or isolation of individuals is a key strategy, the effect of which is in part determined by the network's robustness properties. An example of this is the U.S. government's hope on decapitating Al Qaeda by pursuing high-value targets. In complex network theory it has been shown that networks with a few highly connected nodes (hubs) are resistant to random failures because these hubs dominate their topology (Albert et al. 2000). However, this comes at the cost of vulnerability to deliberate attacks on such hubs. This appears one of the reasons why empirical covert organizations, instead of relying on a few hubs, have evolved into decentralized, non-hierarchical structures as theoretically quantified by our secrecy versus information trade-off performance measure. A case in point is Al Qaeda (Sageman 2008): local groups self-organize by radicalization and interconnect, for instance through the internet. There is no top to bottom leadership or organization. What results is a sparsely connected network safeguarding secrecy, however with low separation (due to the internet's global reach). To understand the resilience of such an organizational form we investigate the effect of the removal of a fraction of vertices of an approximate optimal terrorist network on the basis of the secrecy versus information performance measure. More specifically we compare two scenarios: a fraction f of vertices is either removed randomly from such an approximate optimal terrorist network or the same fraction f being removed consists of vertices with the highest degrees. Results are plotted in Fig.2 (left) in case of random removal and in Fig.2 (right) in case of targeted removal.

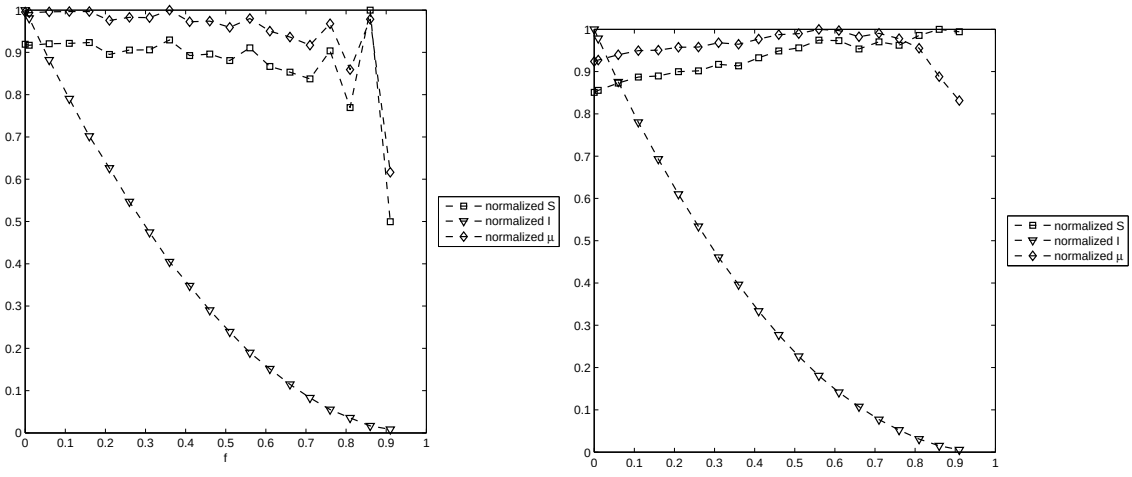

Figure 2: Normalized values of S, I and μ as function of the fraction f of randomly (left) and targeted (right) removed vertices.

From Fig.2 (left) it can be seen that the fraction of randomly removed vertices does not seem to affect the performance of the remaining network structure very much, i.e., μ is only slightly decreasing with increasing values of f. Only after a very large fraction of vertices has been removed ($f \approx 0.75$) does an effect take shape, which can be explained by the disintegration of the network.

Fig.2 (right) on the targeted removal of high degree vertices shows a surprising result. Even though the information measure decreases rapidly with increasing f, the secrecy performance of the organization in fact increases. Balancing these two aspects, the total performance measure μ increases with respect to the fraction f of targeted removals. Thus the more one focuses a destabilization strategy on the targeted removal of central individuals the more a covert organization's capacity to coordinate and control is reduced but the higher its performance in balancing the information versus secrecy trade-off will be. Only at very high values for the fraction $f \approx 0.8$ does the performance measure start to decrease. The implication for terrorist networks is obvious. Their evolution towards global, sparsely connected, leaderless networks has enabled them to survive the continuing targeted attack on their nodes.

Conclusion

By studying terrorist networks from the small-world perspective we shed new light on their structures and the implications this holds for their survival. Since covert organizations are aware of their need to balance secrecy and information, our analysis, using the total performance measure as an evaluation criterion, shows that their network topology will not satisfy a 'small-world' characterization as common in many social systems. In addition we presented empirical evidence to support this claim. That terrorist networks avoid small-world structures can be explained by the low secrecy a highly clustered networked organizational form offers. Another reason for adopting a non small-world topology is found in the remarkable advantage the derived network topology offers against targeted removal. It is known that 'normal' social network topologies will show fast degradation in case of removal of hubs. However we have shown that terrorist networks adopting secrecy and information balanced networks are perfectly capable to outlast targeted attacks. This may partly explain why current transnational terrorist networks appear to be so resilient: as long as disruption strategies do not completely disintegrate the network such efforts only strengthen their ability to attain a balance at remaining secret while being operationally effective...instead of

disabling them to operate at all.

Appendix

A covert network is modeled by a graph $g = (N, E)$, where N represents the set of members (terrorists or terror cells) of the organization and E represents the links among these members. For instance such links may represent the exchange of bomb making material or the communication over the internet. We set $|N| = n$ and $|E| = m$. The set of all such networks is indicated by $\mathbb{G}(n, m)$.

Information measure I

The information measure of a graph $g \in \mathbb{G}(n, m)$ is defined by the normalized reciprocal of the total distance in g, i.e.,

$$I(g) = \frac{n(n-1)}{T(g)}.$$

Here $T(g)$ equals the total geodesic distance, i.e., $T(g) = \sum_{(i,j)\in N^2} l_{ij}(g)$ with $l_{ij}(g)$ the geodesic distance between vertex i and vertex j. It follows that $0 \leq I(g) \leq 1$. Thus the information measure captures the ability of the terrorist organization to exchange information, i.e., to coordinate and control. The higher the value for I the better the organization can do so.

Secrecy measure S

The secrecy measure of a graph $g \in \mathbb{G}(n, m)$ is defined by

$$S(g) = \frac{2m(n-2) + n(n-1) - \sum_{i\in N} d_i^2(g)}{(2m+n)n}.$$

Here $d_i(g)$ equals the degree of vertex i in g. It follows that $0 \leq S(g) \leq 1$. It can be seen that the secrecy measure equals the expected fraction of the organization that survives given that members of the organization are exposed according to a realistically chosen probability distribution.

Balanced trade-off performance measure μ

For $g \in \mathbb{G}(n,m)$ it holds that,

$$\mu(g) = S(g)I(g) = \frac{(n-1)(2m(n-2)+n(n-1)-\sum_{i\in N} d_i^2(g))}{(2m+n)T(g)}.$$

Following multi-objective optimization theory the terrorist organization, faced with trading off secrecy versus information, adopts those values of S and I that maximize their product. For a more thorough motivation of this measure see Lindelauf et al. (2009a).

Small-world indicators

For $g \in \mathbb{G}(n,m)$ the characteristic path length is defined by

$$L(g) = \frac{1}{2}\frac{T(g)}{n(n-1)} = \frac{1}{2I(g)},$$

and the clustering coefficient is defined by,

$$C(g) = \frac{1}{n}\sum_{i\in N} C_i,$$

where

$$C_i = \frac{|N_i(g)|}{|\Gamma_i(g)|(|\Gamma_i(g)|-1)}.$$

Here $\Gamma_i(g) = \{j \in N | l_{ij}(g) = 1\}$ is the set of neighbors of vertex i in network g, and $N_i(g) = \{\{k,l\} \in \Gamma_i(g) | l_{kl}(g) = 1\}$ is the set of neighbor pairs of vertex i that are connected in g. Small-world networks are characterized by low L and high C. When compared to random networks a small-world network satisfies $L \approx L_{random}$ and C is of a different order of magnitude than C_{random}.

Use of normalization

Since only relative comparison plays a role we normalized the indicators I, S, L, C and μ by dividing them by the maximum they attained at each relevant instance. This avoids scaling differences in the corresponding figures but does not affect the resulting analysis.

Generating an approximate optimal covert network

A theoretically optimal covert network was approximated on $n = 100$ individuals as follows. We let $p \in \{0.3, 0.4, 0.5, 0.6, 0.7\}$ and for each fixed p we generated 100.000 random graphs with each

possible edge present independently and identically distributed with probability p. Among these 500.000 networks the one that attained the highest value for μ was selected.

References:

Albert, R., Jeong, H., Barabsi, A.-L. Error and attack tolerance of complex networks. *Nature* **406**: 378-482 (2000).

Arquilla, J., Ronfeldt, D. *Networks and netwars: the future of terror, crime and militancy* (Santa Monica, Calif. :RAND, 2001).

Asal, V., Nussbaum, B. & Harrington D.W. Terrorism as Transnational Advocacy: An Organizational and Tactical Examination. *Studies in Conflict & Terrorism* **30**: 15-39 (2007).

Bergen, P. The Osama Bin Laden I Know: An Oral History of al Qaedas Leader. Free Press, New York (2006).

Borgatti, S.P. The Key Player Problem (Proceedings from National Academy of Sciences Workshop on Terrorism, Washington DC 2002).

Carley, K.M. Destabilization of covert networks. *Computational & Mathematical Organization Theory* **12**(1): 51-66 (2006).

Enders, W. & Su, X. Rational Terrorists and Optimal Network Structure. *Journal of Conflict Resolution* **51**(1): 33-57 (2007).

Farley, J.D. Breaking Al Qaeda Cells: a Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Management and Decision Making). *Studies in Conflict and Terrorism* **26**: 399-411 (2003).

Jasny, B.R. & Ray, B. Life and the Art of Networks. *Science* **301**: 1863 (2003).

Koschade, S. A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence. *Studies in Conflict & Terrorism* **29**: 559-575 (2006).

Lindelauf, R., Borm, P. & Hamers, H. The Influence of Secrecy on the Communication Structure of Covert Networks. *Social Networks* **31**: 126-137 (2009a).

Lindelauf, R.H.A., Borm, P.E.M., Hamers, H.J.M. in Mathematical Methods in Counter-terrorism (eds Memon, N., Farley, J.D., Hicks, D.L. & Rosenorn, T.) On Heterogeneous Covert Networks (Springer-Verlag 2009b).

Magouirk, J. et al. Connecting Terrorist Networks. *Studies in Conflict & Terrorism* **31**: 1-16 (2008).

McCormick, G.H. & Owen, G. Security and Coordination in a Clandestine Organization. *Mathe-*

matical and Computer Modelling **31**: 175-192 (2000).

Morselli, K., Petit, K. & Giguere, C. The efficiency/security trade-off in criminal networks. *Social Networks* **29**: 143-153 (2007).

Natarajan, M. Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data. *J. Quant. Criminol.* **22**: 171-192 (2006).

Newman, M., Barabasi, A.L. & Watts, D.J. *The Structure and Dynamics of Networks* (Princeton University Press, Princeton, 2006).

Sageman, M. *Leaderless Jihad: Terror Networks in the Twenty-first Century* (University of Pennsylvania Press, Philadelphia, 2008).

Sparrow, M. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* **13**: 251-274 (1991).

Strogatz, S.H. Exploring complex networks. *Nature* **410**: 268-276 (2001).

Wasserman

Watts, D.J. & Strogatz, S.H. Collective Dynamics of 'small-world' networks. *Nature* **393**: 440-442 (1998).

Watts, D.J. The 'New' Science of Networks. *Annu. Rev. Sociol.* **30**: 243-70 (2004).

Zacharias, G.L. et al. *Behavioural Modelling and Simulation: From Individuals to Societies* (National Academy of Sciences, Washington D.C., 2008).